Kroll | A Division of DUFF & PHELPS

INFINITE GLOBAL

Mitigating Reputational Risk & Restoring Customer Trust:

Optimizing the Role of PR In Data Breach Response

Brian Lapidus, Practice Leader, Identity Theft & Breach Notification, Kroll

Zach Olsen, President, Infinite Global

Kelsey Eidbo, Client Supervisor, Infinite Global

It’s rough out there…

22 Million
PII
2012 - 2014
Security clearance
information part of the breach

110 Million
Credit cards
2013
$162 Million
estimated cost of the breach

3 Billion
User accounts
2013-2014
$350 Million
est. decrease in sale price to Verizon

145 Million
User accounts
2014
Days: 229
hackers had access to internal data

83 Million
Contact Information
2014
$250 Million
spent on security annually

143 Million
PII
2017
2+ months
est. time to discover the breach

SOURCE: The 16 biggest data breaches of the 21st century, CSO, October 11, 2017

And the incident is just the beginning…

REMEDIATION

BUSINESS DISRUPTION

CUSTOMER CHURN

FINES

LEGAL COSTS

BRAND REPUTATION

FINANCIAL LOSS

NOTIFICATION COSTS

ONGOING MONITORING

… but a strong communications plan can help here:

REMEDIATION

BUSINESS DISRUPTION

CUSTOMER CHURN

FINES

LEGAL COSTS

BRAND REPUTATION

FINANCIAL LOSS

NOTIFICATION COSTS

ONGOING MONITORING

… and potentially here:

REMEDIATION

BUSINESS DISRUPTION

CUSTOMER CHURN

FINES

LEGAL COSTS

BRAND REPUTATION

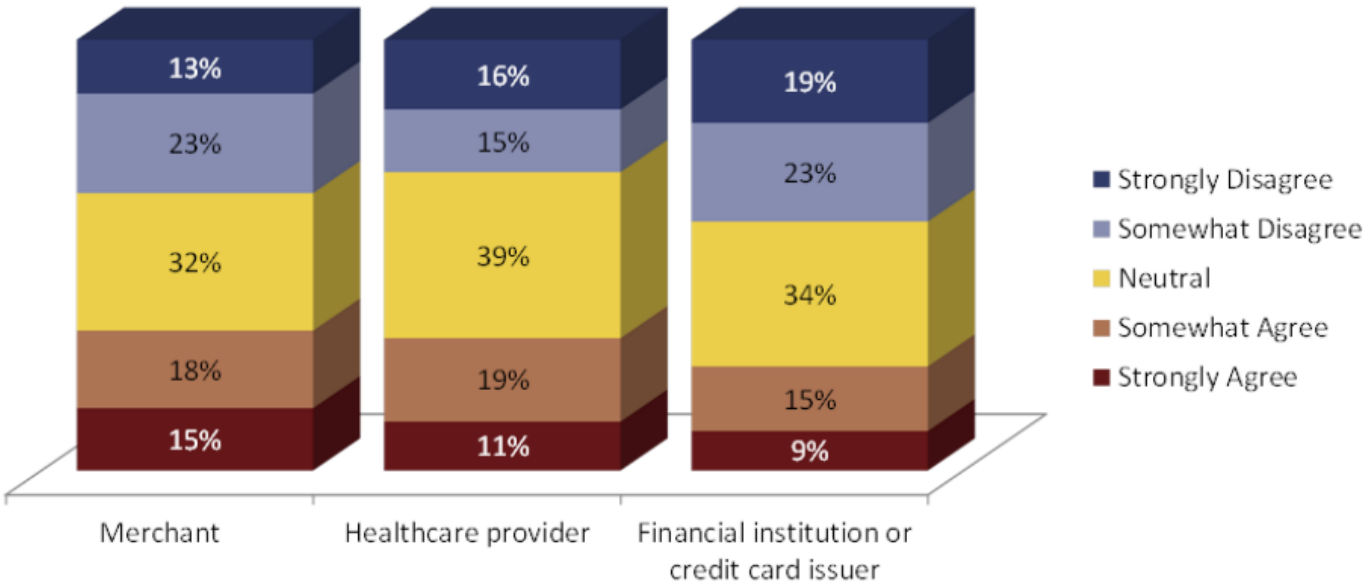
FINANCIAL LOSS

NOTIFICATION COSTS

ONGOING MONITORING

Data Breaches Can Cause Customer Churn

Figure 1: Avoidance of Further Business, by Type of Organization in Which Data Breach Occurred



Q2D. Please indicate the type of organization where the data breach occurred.
Q2K. Please read each of the following statements carefully and indicate your level of agreement ("I avoid doing further business with the organization(s)" shown).

October 2013, n = varies: 111 – 897
Base: All consumers whose PII was breached at an FI or CC issuer, All consumers whose PII was breached at a merchant, All consumers whose PII was breached at a healthcare provider

Crisis communications is part of a defensible security strategy

Pre-breach Communications Planning

- Find an experienced outside public relations team, get to know them ahead of an incident, and introduce them to your in-house response team.
- Develop a crisis communications playbook that covers (at minimum):
  - The crisis communications team and contact information for all members (in-house and external)
  - Internal and external audiences
  - Media policies to be distributed firm-wide before an incident and on a regular basis.
  - Contact information of key journalists
- Run a tabletop exercise with all crisis communications team members
- Keep your plan, and the people involved, fresh

Responding to a Breach: The Role of PR

A good PR firm will help an organization:

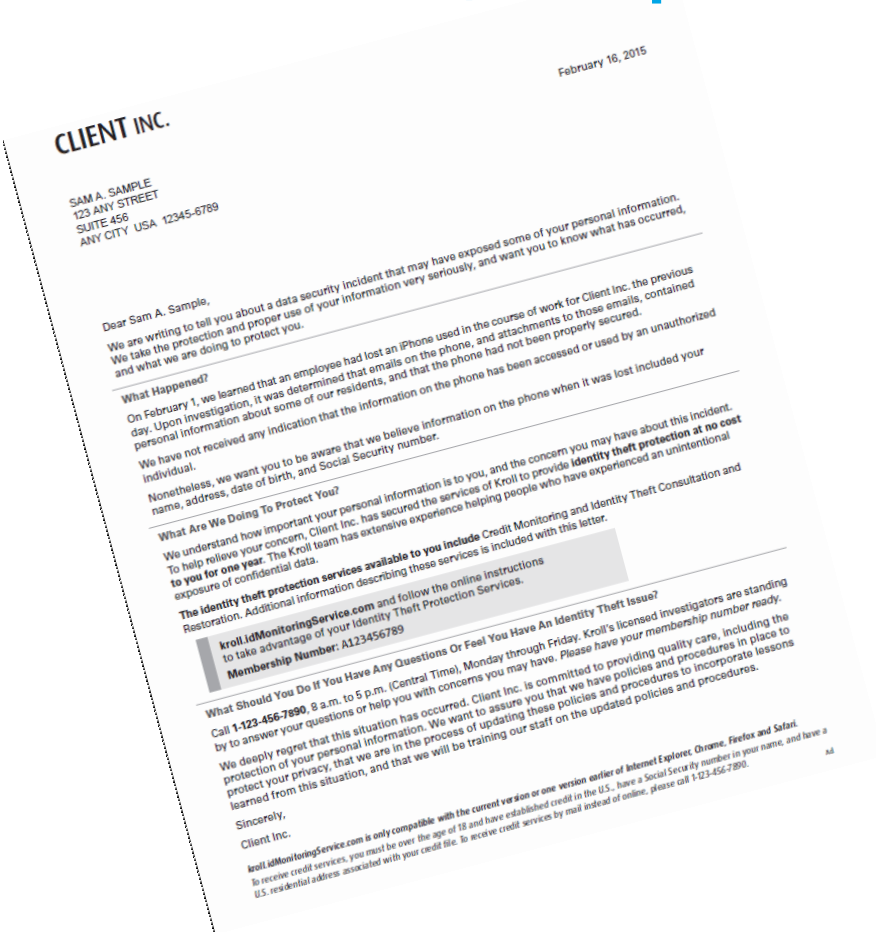
- Understand the media landscape that is specific to them and their industry
- The media cycle of a data breach
- How to communicate to critical audiences throughout a breach
- When and how to leverage social media
- Managing the expectations of “interested” vs. “affected” parties
- Maintain consistency of messaging when communicating across various platforms
- When to be proactive, reactive or quiet

Responding to a Breach: The Role of PR – cont'd

A good PR firm will help an organization:

- Anticipate the next phase of the news cycle, and advise on how to plan and react
- Determine "best case" and "worst case" scenarios provide counsel on how to proactively address internal questions
- Control the pace with which media is responded to
- Liaise between legal team and client to ensure all communications – internal and external – are meeting the needs and goals of all parties

Customized, Compliant Communications



CLIENT INC.

February 16, 2015

SAM A. SAMPLE
123 ANY STREET
SUITE 456
ANY CITY USA 12345-6789

Dear Sam A. Sample,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously, and want you to know what has occurred, and what we are doing to protect you.

What Happened?

On February 1, we learned that an employee had lost an iPhone used in the course of work for Client Inc. the previous day. Upon investigation, it was determined that emails on the phone, and attachments to those emails, contained personal information about some of our residents, and that the phone had not been properly secured.

We have not received any indication that the information on the phone has been accessed or used by an unauthorized individual.

Nonetheless, we want you to be aware that we believe information on the phone when it was lost included your name, address, date of birth, and Social Security number.

What Are We Doing To Protect You?

We understand how important your personal information is to you, and the concern you may have about this incident. To help relieve your concern, Client Inc. has secured the services of Kroll to provide **identity theft protection at no cost to you for one year**. The Kroll team has extensive experience helping people who have experienced an unintentional exposure of confidential data.

The identity theft protection services available to you include Credit Monitoring and Identity Theft Consultation and Restoration. Additional information describing these services is included with this letter.

What Should You Do If You Have Any Questions Or Feel You Have An Identity Theft Issue?

Call **1-123-456-7890**, 8 a.m. to 5 p.m. (Central Time), Monday through Friday. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. *Please have your membership number ready.*

We deeply regret that this situation has occurred. Client Inc. is committed to providing quality care, including the protection of your personal information. We want to assure you that we have policies and procedures in place to protect your privacy, that we are in the process of updating these policies and procedures to incorporate lessons learned from this situation, and that we will be training our staff on the updated policies and procedures.

Sincerely,

Client Inc.

kroll.idMonitoringService.com is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. To receive credit services by mail instead of online, please call 1-123-456-7890.

kroll.idMonitoringService.com and follow the online instructions

Membership Number: A123456789

- **When/Where did the theft/breach occur?**
- **What happened? What was lost or stolen?**
- **What is [CLIENT] doing about this?**
  *[**SAMPLE**: Client immediately notified local law enforcement and is cooperating with them as they continue their investigation.]*
- **What is [CLIENT] doing to prevent this from happening in the future?**
  *[**SAMPLE**: [CLIENT] has examined and analyzed existing procedures and systems to ensure appropriate security measures are (reinforced/in place).]*
- **Why wasn't I notified sooner?**
  *[**SAMPLE**: [CLIENT] immediately notified local law enforcement officials and launched an investigation into the incident. The investigation included a review of internal security systems to confirm that procedures already in place are strengthened to further safeguard against a breach of data security in the future. Last, it was imperative that impacted individuals were identified and their contact information gathered into a consistent format for notification. This investigation was a time-consuming process, but Client believed it was necessary to ensure appropriate precautions and next steps were taken.]*

How it Works – Breach Notification

- Distill the data for optimized mail delivery
  - Standardize addresses, report and remedy exceptions
  - Sort and group special populations
  - Compare against NCOA database
  - Dedicate a toll-free telephone number; include in notice
- Draft notification letter(s) congruent with state law(s) and audience(s)
  - Include clear guidelines about how to use any services offered to help mitigate identity theft fears and threats
- Monitor and report on returned mail

Consider: Proof that Stands Up Later

Case Studies

- Case #1: Rapid, Large-scale Response
  - Onsite implementation, ready to be on ground in 48 hours,
  - Multiple letter versions
  - Banner on Kroll.com homepage to steer people to public notice page

- Case #2: Supporting clients in litigation following an event
  - Supplied post-event reporting, documentation, and recorded calls
  - Provided onsite deposition and case preparation data to help demonstrate the expertise of the services provided to notification subjects

Kroll | A Division of DUFF & PHELPS

INFINITE GLOBAL

Q&A

Contact Details

Brian Lapidus
Practice Leader
Identity Theft and Breach Notification
T + 1 615.577.6770

blapidus@kroll.com

Kelsey Eidbo
Client Supervisor

T +1 415.732.7804

kelseye@infiniteglobal.com

Zach Olsen
President

T +1 415.732.7802

zach@infiniteglobal.com